CERT-MU Advisory

CERT-MU

Following the Security Alert sent by CERT-MU on 27th June 2017, please find below the advisory on the Petya Global Ransomware Attack:

The Massive Petya Global Ransomware Attack

Original Issue Date: 27th June 2017

Severity Rating: High

Description:

A major Ransomware Cyber Attack known as **"Petya"** is creating havoc across the world. Many critical systems, organisations, airports, banks and Government departments in Europe as well as in other countries have already been affected. The new variant of the Petya Ransomware is spreading rapidly with the help of same Windows SMBv1 vulnerability that the WannaCry Ransomware exploited and uses the NSA EternalBlue Exploit.

Affected Systems:

Windows XP through 8.1 which do not have the latest security updates are at risk of infection. (Windows 10 is not vulnerable).

Methodology of Attack:

1. Petya uses the NSA Eternalblue exploit but also spreads in internal networks with Windows Management Instrumentation Command-line (WMIC) and PsEXEC.
2. The Ransomware works differently from any other ransomware malware. Unlike other traditional ransomware, Petya does not encrypt files on a targeted system one by one.
3. Instead, Petya reboots victims computers and encrypts the hard drive's master file table (MFT) and renders the master boot record (MBR) inoperable, restricting access to the full system by seizing information about file names, sizes, and location on the physical disk.

4. Then the Petya ransomware replaces the computer's MBR with its own malicious code that displays the ransom note, demanding $300 in Bitcoins and leaves computers unable to boot.

Precautions to be taken to protect from this ransomware campaign:

- Aggressively **patch and update** Anti-Virus signatures (including MS17-010).
- Warn users **not to open attachments/enable macros** on suspicious emails. This may be the entry vector so diligence is warranted
- If you suspect you may be a victim, install Windows Defender; and run to remove the malware on systems
- If patching is not possible (i.e. if the machines cannot be updated with the March MS17-010), temporarily block SMB connections to limit the spread. This will likely impact your organization's services. The following workarounds may be helpful in your situation:
    - Disable SMBv1
    - For customers running Windows Vista and later, see Microsoft Knowledge Base Article 2696547.

Users are strongly recommended not to pay the ransom. Encrypted files should be restored from back-ups where possible.

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu